REMARKS

Claims 1-15 are pending. Reconsideration and allowance of the present application based on the following remarks are respectfully requested.

Claims Rejections Under 35 U.S.C. § 102(e)

Claims 1-15 were rejected under 35 U.S.C. § 102(e) over Buttiker (U.S. Publication No. 2002/0176583). Applicants respectfully traverse this rejection.

Claim 1 recites a method for modifying validity of a certificate using biometric information in a public key infrastructure-based authentication system that includes accessing a server of the certificate authority using login information of the user in response to a certificate validity modification request from the user under the condition that he/she is registered as a member in the authentication system; inputting the biometric information for a user authentication through a biometric information input unit in the user system; generating a certificate validity modification request message in response to the certificate validity modification request from the user; and sending the inputted biometric information and the generated certificate validity modification request message to the certificate authority to request the certificate validity modification online.

As discussed previously, Buttiker is directed to a process and to an end objective that are completely distinct from those to which the pending application is directed. In particular, while the pending claims of the present application are directed to a method for modifying online the validity of certificates by users who are registered members of a PKI-based authentication system, Buttiker pertains exclusively to a system, method and token for registering new users to a public key infrastructure (PKI) system.

In Applicants' response to the last office action, Applicants argued that Buttiker discloses only registering of new users and not of modifying validity of certificates. To this argument, the Examiner responds that Buttiker discloses "validation of certificates" in paragraphs [0014] and [0017]. However, validating a certificate is not the same modifying the validity of a certificate. Validating a certificate is merely the result of a certification. More particularly, "[w]hen a certifying authority certifies an entity and a user then validates that certification, the entity is said to have been authenticated." (Para. [0017]). In the words, the user is merely checking whether a certificate is valid. The validity of the certificate is not changed.

The Examiner further argues that Buttiker discloses "maintaining a directory containing revoked certificates" in para. [0047]. However, Buttiker nowhere discloses that the revoked

certificates were revoked by using a certificate validity modification request containing biometric information, as required by claim 1.

Finally, the Examiner states that the "functions of the token containing certificates" include "invalidating/revoking the token/certificates." First, the Examiner states that tokens contain certificates. This is incorrect. Figure 1 shows a token 10. There is no certificate in token 10. Referring to figure 2, certificates are managed by the authority 100. This is made clear by paragraph [0016], which states "in other words a certificate is therefore an encrypted message issued by the certification authority declaring that the therein contained public-key relates to the enclosed subject identification information." Second, the Examiner states that "functions of a token" include "invalidating/revoking the token/certificates." Paragraph [0062], o which the Examiner cites, provides no support for this contention. Applicants submit that Buttiker nowhere discloses what the "functions of the token" are. To the extent the Examiner is relying on an inherency argument in this instance, the Examiner has not carried the burden of demonstrating that "functions of the token" include revoking certificates. MPEP 2112(IV). Third, even if paragraph [0062] inherently discloses comparing biometric data of a user to stored biometric data before revoking a certificate, Buttiker does so in a different manner than claimed in claim 1. Paragraph [0062] states that biometric data is stored in memory device 5 of token 10. Before allowing access to the "functions of the token 10," biometric data entered on biometric input device 1 or 31 is compared to the biometric data stored in memory device 5 of token 10. In claim 1 on the other hand, "inputted biometric information and the generated certificate modification request message" are sent to the **certificate authority**. Buttiker does the comparison of paragraph [0062] inside the token 10.

Referring back to the language of claim 1, Buttiker indisputably does not disclose "sending the inputted biometric information and the generated certificate validity modification request message to the certificate authority" because Buttiker nowhere discloses a "certificate validity **modification** message." The Examiner cites to paragraph [0054] for this element, but this paragraph only discloses certificate registration, not certificate modification. The Examiner appears to ultimately be relying on an inherency argument, in that Buttiker discloses revoked certificates, and it discloses registration of certificates using biometric information, so therefore it must disclose certificate modification using biometric information. However, this argument cannot be made without the Examiner first establishing that the "missing descriptive matter is **necessarily** present in the thing described in the reference." MPEP 2112(IV) (emphasis added). The Examiner has not done so.

Accordingly, Buttiker fails to teach, or even suggest, a method for modifying validity of a certificate using biometric information in a public key infrastructure-based authentication system that includes accessing a server of the certificate authority using login information of the user in response to a certificate validity modification request from the user under the condition that he/she is registered as a member in the authentication system; inputting the biometric information for a user authentication through a biometric information input unit in the user system; generating a certificate validity modification request message in response to the certificate validity modification request from the user; and sending the inputted biometric information and the generated certificate validity modification request message to the certificate authority to request the certificate validity modification online, as recited in claim 1.

Claim 3 is believed allowable for at least the same reasons presented above with respect to claim 1 since claim 3 recites features that are similar to the features of claim 1 discussed above.

Claims 2 and 4-15 are believed allowable for at least the same reasons presented above with respect to claims 1 and 3 by virtue of their dependence upon claims 1 and 3. Accordingly, Applicants respectfully request reconsideration and withdrawal of this rejection.

Conclusion

Therefore, all objections and rejections having been addressed, it is respectfully submitted that the present application is in a condition for allowance and a Notice to that effect is earnestly solicited.

Should any issues remain unresolved, the Examiner is encouraged to contact the undersigned attorney for Applicants at the telephone number indicated below in order to expeditiously resolve any remaining issues.

Respectfully submitted,

MAYER BROWN ROWE & MAW LLP

By: _____

Yoon S. Ham
Registration No. 45,307
Direct No. (202) 263-3280

YSH/NH
Intellectual Property Group
1909 K Street, N.W.
Washington, D.C. 20006-1101
(202) 263-3000 Telephone
(202) 263-3300 Facsimile

Date: January 24, 2007